張貼日期：2025/10/09

# 【漏洞預警□CISA新增10個已知遭駭客利用之漏洞至KEV目錄(2025/09/29-2025/10/05)

- 主旨說明:【漏洞預警□CISA新增10個已知遭駭客利用之漏洞至KEV目錄(2025/09/29-2025/10/05)

- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202510-00000003

1. □CVE-2025-32463□Sudo Inclusion of Functionality from Untrusted Control Sphere Vulnerability (CVSS v3.1: 9.3)
   - 【是否遭勒索軟體利用:未知□ Sudo 1.9.17p1之前的版本存在漏洞，允許本地使用者取得root權限，原因在於使用–chroot選項時，會使用來自使用者可控目錄的/etc/nsswitch.conf檔案。
   - 【影響平台】請參考官方所列的影響版本
   - https://www.sudo.ws/security/advisories/chroot_bug/
2. □CVE-2025-59689□Libraesva Email Security Gateway Command Injection Vulnerability (CVSS v3.1: 6.1)
   - 【是否遭勒索軟體利用:未知□ Libraesva Email Security Gateway (ESG)存在指令注入漏洞，允許透過壓縮的電子郵件附件執行指令注入攻擊。
   - 【影響平台】請參考官方所列的影響版本
   - https://docs.libraesva.com/knowledgebase/security-advisory-command-injection-vulnerability-cve-2025-59689/
3. □CVE-2025-10035□Fortra GoAnywhere MFT Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 10.0)
   - 【是否遭勒索軟體利用:已知□ Fortra GoAnywhere MFT存在反序列化不受信任資料漏洞，允許攻擊者偽造合法的授權回應簽章，反序列化任意由其控制的物件，可能導致指令注入。
   - 【影響平台】請參考官方所列的影響版本
   - https://www.fortra.com/security/advisories/product-security/fi-2025-012
4. □CVE-2025-20352□Cisco IOS and IOS XE Software SNMP Denial of Service and Remote Code Execution Vulnerability (CVSS v3.1: 7.7)
   - 【是否遭勒索軟體利用:未知□ Cisco IOS與IOS XE在SNMP子系統中存在堆疊緩衝區溢位漏洞，可能導致拒絕服務(DoS)或遠端程式碼執行。
   - 【影響平台】請參考官方所列的影響版本
   - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte
5. □CVE-2021-21311□Adminer Server-Side Request Forgery Vulnerability (CVSS v3.1: 7.2)
   - 【是否遭勒索軟體利用:未知□ Adminer存在伺服器端請求偽造(SSRF)漏洞，該漏洞若被利用，將允許遠端攻擊者取得潛在敏感資訊。
   - 【影響平台】請參考官方所列的影響版本
   - https://github.com/vrana/adminer/security/advisories/GHSA-x5r2-hj5c-8jx6
6. □CVE-2014-6278□GNU Bash OS Command Injection Vulnerability (CVSS v3.1: 8.8)
   - 【是否遭勒索軟體利用:未知□ GNU Bash存在作業系統指令注入漏洞，允許遠端攻擊者透過特製的環境變數執行任意指令。
   - 【影響平台□ GNU Bash 1.14至4.3(含)的版本
7. □CVE-2017-1000353□Jenkins Remote Code Execution Vulnerability (CVSS v3.1: 9.8)

    - 【是否遭勒索軟體利用:未知】 Jenkins存在遠端程式碼執行漏洞。此漏洞允許攻擊者將序列化的Java SignedObject物件傳輸至基於遠端通訊的Jenkins CLI，該物件將透過新的ObjectInputStream進行反序列化，從而繞過現有的基於封鎖清單的防護機制。
    - 【影響平台】請參考官方所列的影響版本
    - https://www.jenkins.io/security/advisory/2017-04-26/
8. 【CVE-2015-7755】Juniper ScreenOS Improper Authentication Vulnerability (CVSS v3.1: 9.8)
    - 【是否遭勒索軟體利用:未知】 Juniper ScreenOS存在不當驗證漏洞，可能允許未經授權的遠端管理存取該設備。
    - 【影響平台】請參考官方所列的影響版本
    - https://supportportal.juniper.net/s/article/2015-12-Out-of-Cycle-Security-Bulletin-ScreenOS-Multiple-Security-issues-with-ScreenOS-CVE-2015-7755-CVE-2015-7756
9. 【CVE-2025-21043】Samsung Mobile Devices Out-of-Bounds Write Vulnerability (CVSS v3.1: 8.8)
    - 【是否遭勒索軟體利用:未知】 三星行動裝置在libimagecodec.quram.so中存在越界寫入漏洞，允許遠端攻擊者執行任意程式碼。
    - 【影響平台】請參考官方所列的影響版本
    - https://security.samsungmobile.com/securityUpdate.smsb
10. 【CVE-2025-4008】Smartbedded Meteobridge Command Injection Vulnerability (CVSS v3.1: 8.8)
    - 【是否遭勒索軟體利用:未知】 Smartbedded Meteobridge 存在指令注入漏洞，可能允許未經身分驗證的遠端攻擊者在受影響的裝置上以提升權限(root)執行任意指令。
    - 【影響平台】請參考官方所列的影響版本
    - https://forum.meteohub.de/index.php

- 影響平台:
    - 詳細內容於內容說明欄之影響平台
- 建議措施:
1. 【CVE-2025-32463】 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://www.sudo.ws/security/advisories/chroot_bug/
2. 【CVE-2025-59689】 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://docs.libraesva.com/knowledgebase/security-advisory-command-injection-vulnerability-cve-2025-59689/
3. 【CVE-2025-10035】 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://www.fortra.com/security/advisories/product-security/fi-2025-012
4. 【CVE-2025-20352】 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte
5. 【CVE-2021-21311】 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://github.com/vrana/adminer/security/advisories/GHSA-x5r2-hj5c-8jx6
6. 【CVE-2014-6278】 漏洞可能影響開源元件、第三方函式庫、協定或特定實作。請依照產品釋出之緩解措施進行修補。
7. 【CVE-2017-1000353】 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://www.jenkins.io/security/advisory/2017-04-26/
8. 【CVE-2015-7755】 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://supportportal.juniper.net/s/article/2015-12-Out-of-Cycle-Security-Bulletin-ScreenOS-Multiple-Security-issues-with-ScreenOS-CVE-2015-7755-CVE-2015-7756
9. 【CVE-2025-21043】 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://security.samsungmobile.com/securityUpdate.smsb
10. 【CVE-2025-4008】 官方已針對漏洞釋出修復更新，請更新至相關版本
    - https://forum.meteohub.de/index.php

計算機與通訊中心
網路系統組 敬啟